WHAT IS CLAIMED IS:

1. An apparatus for encrypting block data comprising:

encrypting sections connected in series, each of the encrypting sections comprising:

a first unit configured to randomize first subblock data which are obtained by dividing the block data; and

a second unit configured to diffuse data output from the first unit with respect to a range which is wider than a range of the first subblock data and supply a result of diffusion to a first unit in a succeeding encrypting section, at least one bit of data input to the first unit in own encrypting section being transmitted to at least one bit of data input to the first unit in the succeeding encrypting section via at least two routes.

2. The apparatus according to claim 1, wherein the at least one bit is present in each of the block data.

3. The apparatus according to claim 1, wherein, for each of all combinations of one bit selected from the data input to the first unit in the own encrypting section and one bit selected from the block data input to the first unit in the succeeding encrypting section or for some of the combinations which meet a predetermined condition, one bit of the data input to

the first unit in the own encrypting section is transmitted to one bit of the data input to the first unit in the succeeding encrypting section via at least two routes.

4. An apparatus for encrypting block data comprising:

encrypting sections connected in series, each of the encrypting sections comprising:

first nonlinear transformation units configured to perform a nonlinear transformation process over first subblock data which are obtained by dividing the block data; and

a first linear diffusion unit configured to perform a linear diffusion process over data output from the first nonlinear transformation units with respect to a range which is wider than a range of the first subblock data and supply a result of diffusion to first nonlinear transformation units in a succeeding encrypting section,

wherein each of the first nonlinear transformation units comprises:

second nonlinear transformation units configured to perform a nonlinear transformation process over second subblock data which are obtained by dividing the first subblock data; and

a second linear diffusion unit configured to perform a linear diffusion process over data output

from the second nonlinear transformation units with respect to the range of the first subblock data, and

wherein at least one bit of data input to one of the second nonlinear transformation units in each of the encrypting sections is transmitted to at least one bit of data input to one of the second nonlinear transformation units in the succeeding encrypting section via at least two routes.

5. The apparatus according to claim 4, wherein

the second nonlinear transformation unit in the first nonlinear transformation unit comprises a first-half second nonlinear transformation units preceding the second linear diffusion unit and second-half second nonlinear transformation units succeeding the second linear diffusion unit, and

the first linear diffusion unit in each of the encrypting sections supplies an exclusive OR value of at least two outputs from the second-half second nonlinear transformation units to at least one input to the first-half second nonlinear transformation units in the succeeding encrypting section.

6. The apparatus according to claim 4, wherein

the second nonlinear transformation unit in the first nonlinear transformation unit comprises a first-half second nonlinear transformation units preceding the second linear diffusion unit and second-half second nonlinear transformation units succeeding the second

linear diffusion unit, and

the first linear diffusion unit in each of the encrypting sections supplies each exclusive OR value of at least two outputs from the second-half second nonlinear transformation units to each input to the first-half second nonlinear transformation units in the succeeding encrypting section.

7. The apparatus according to claim 4, wherein

each of the first subblock data has equal bit length and each of the second subblock data has equal bit length, and

the first linear diffusion unit performs a linear diffusion process on a bit group formed of corresponding bits each extracted from a respective one of the second subblock data while changing a bit extracted position.

8. The apparatus according to claim 7, wherein the block data is 128 bits in length, each of the first subblock data is 32 bits in length, and each of the second subblock data is 8 bits in length,

the first linear diffusion unit performs a linear diffusion process on eight 16-bit data formed of corresponding bits each extracted from a respective one of sixteen second subblock data while changing a bit extracted position.

9. The apparatus according to claim 4, wherein the first linear diffusion unit is implemented by

hardware.

10. The apparatus according to claim 9, wherein an input-output characteristic of the first linear diffusion unit is based on multiplication over the Galois field.

11. The apparatus according to claim 5, wherein the first linear diffusion unit is implemented by software.

12. An encryption apparatus based on a block encryption scheme comprising:

encrypting sections connected in series in which the first section receives 128-bit plaintext and each of the second section and later sections receives 128-bit block data processed by the preceding section, each of the encrypting sections comprising four first nonlinear transformation units each of which performs a local linear diffusion process and a nonlinear transformation process a corresponding one of four sets of 32-bit data into which 128-bit block data is divided; and a first diffusion unit for performing a linear diffusion process using a maximum distance separable matrix on 128-bit block data in which four sets of 32-bit data output from the four first nonlinear transformation units are concatenated and outputting the processed 128-bit block data to the next stage;

four first nonlinear transformation units which

are connected to first diffusion unit in the last encryption unit and receive 128-bit block data output from the first diffusion unit; and

a first key addition unit configured to receive four sets of 32-bit data output from the four first nonlinear transformation units and output 128-bit encrypted block data by adding 128-bit extended key data to 128-bit block data which is obtained by concatenating the four sets of 32-bit data output from those four first nonlinear transformation units,

wherein each of the first nonlinear transformation units comprises four second key addition units each of which adds 8-bit key data to a corresponding one of four sets of 8-bit data into which the 32-bit data is divided, four second nonlinear transformation units each of which performs nonlinear transformation on a corresponding one of the outputs of the second key addition units, a second diffusion unit for performing a linear diffusion process using a maximum distance separable table on 32-bit data obtained by concatenating the four sets of 8-bit data output from the four second nonlinear transformation units, and four sets of third key addition units and a third nonlinear transformation units connected to follow the second diffusion unit,

each of the first diffusion unit comprises a 16-bit diffusion unit for each of 8 bits for the second

nonlinear transformation units in preceding and succeeding stages, the 16-bit diffusion unit performing a linear diffusion process through a 4 × 4 matrix operation based on multiplication over the Galois field GF(2^4) or its equivalent circuit, the matrix operation being such that four bits at corresponding bits positions in four sets of 8-bit data from the four second nonlinear transformation units in one first nonlinear transformation section in the preceding stage are taken as one element on the input side of the matrix operation and four bits at corresponding bit positions in four sets of 8-bit data input to the four second nonlinear transformation section in one first nonlinear transformation processing section in the succeeding stage are taken as one element on the output side of the matrix operation, and

in the 4 × 4 matrix operation based on multiplication over the Galois field GF(2^4) in the 16-bit diffusion unit or its equivalent circuit transmitting, in any combination of one bit in the outputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the preceding stage and one bit in the inputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the succeeding stage, the state of that one bit in the

preceding stage to that one bit in the succeeding stage is transmitted over a plurality of operations paths.

13. An encryption apparatus based on common-key block encryption scheme comprising:

encrypting sections connected in series in which the first section receives 64-bit plaintext and each of the second section and later sections receives 64-bit block data processed by the preceding section, each of the encrypting sections comprising two first nonlinear transformation units each of which performs a local linear diffusion process and a nonlinear transformation process a corresponding one of two sets of 32-bit data into which 64-bit block data is divided; and a first diffusion unit for performing a linear diffusion process using a maximum distance separable matrix on 64-bit block data in which two sets of 32-bit data output from the two first nonlinear transformation units are concatenated and outputting the processed 64-bit block data to the next stage;

four first nonlinear transformation units which are connected to first diffusion unit in the last encryption unit and receive 64-bit block data output from the first diffusion unit; and

a first key addition unit configured to receive two sets of 32-bit data output from the two first nonlinear transformation units and output 64-bit encrypted block data by adding 64-bit common key data

to 64-bit block data which is obtained by concatenating the two sets of 32-bit data output from those two first nonlinear transformation units,

wherein each of the first nonlinear transformation units comprises four second key addition units each of which adds 8-bit key data to a corresponding one of four sets of 8-bit data into which the 32-bit data is divided, four second nonlinear transformation units each of which performs nonlinear transformation on a corresponding one of the outputs of the second key addition units, a second diffusion unit for performing a linear diffusion process using a maximum distance separable table on 32-bit data obtained by concatenating the four sets of 8-bit data output from the four second nonlinear transformation units, and four sets of third key addition units and a third nonlinear transformation units connected to follow the second diffusion unit,

each of the first diffusion unit comprises a 16-bit diffusion unit for each of 8 bits for the second nonlinear transformation units in preceding and succeeding stages, the 16-bit diffusion unit performing a linear diffusion process through a 2 × 2 matrix operation based on multiplication over the Galois field GF(2^4) or its equivalent circuit, the matrix operation being such that four bits at corresponding bits positions in four sets of 8-bit data from the four

second nonlinear transformation units in one first nonlinear transformation section in the preceding stage are taken as one element on the input side of the matrix operation and four bits at corresponding bit positions in four sets of 8-bit data input to the four second nonlinear transformation section in one first nonlinear transformation processing section in the succeeding stage are taken as one element on the output side of the matrix operation, and

in the 2 × 2 matrix operation based on multiplication over the Galois field GF(2^4) in the 16-bit diffusion unit or its equivalent circuit transmitting, in any combination of one bit in the outputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the preceding stage and one bit in the inputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the succeeding stage, the state of that one bit in the preceding stage to that one bit in the succeeding stage is transmitted over a plurality of operations paths.

14. A method for encrypting block data comprising:

randomizing first subblock data which are obtained by dividing the block data;

diffusing the randomized data with respect to a range which is wider than a range of the first subblock

data;

repeating the randomizing and the diffusing, wherein at least two bits of the randomized data is reflected on one bit of data to be randomized next.

15. An article of manufacture comprising a computer readable medium having a computer program embodied therein, the computer program comprising:

computer readable program code means for causing a computer to randomize first subblock data which are obtained by dividing plaintext block data;

computer readable program code means for causing a computer to diffuse the randomized data with respect to a range which is wider than a range of the first subblock data; and

computer readable program code means for causing a computer to repeat the randomizing and the diffusing, wherein at least two bits of the randomized data is reflected on one bit of data to be randomized next.

16. An apparatus for decrypting encrypted block data comprising:

decrypting sections connected in series, each of the decrypting sections comprising:

a first unit configured to randomize first subblock data which are obtained by dividing encrypted block data; and

a second unit configured to diffuse data output from the first unit with respect to a range which is

wider than a range of the first subblock data and supply a result of diffusion to a first unit in a succeeding encrypting section, at least one bit of data input to the first unit in own encrypting section being transmitted to at least one bit of data input to the first unit in the succeeding encrypting section via at least two routes.

17. A method for decrypting encrypted block data comprising:

randomizing first subblock data which are obtained by dividing encrypted block data;

diffusing the randomized data with respect to a range which is wider than a range of the first subblock data;

repeating the randomizing and the diffusing, wherein at least two bits of the randomized data is reflected on one bit of data to be randomized next.

18. An article of manufacture comprising a computer readable medium having a computer program embodied therein, the computer program comprising:

computer readable program code means for causing a computer to randomize first subblock data which are obtained by dividing encrypted block data;

computer readable program code means for causing a computer to diffuse the randomized data with respect to a range which is wider than a range of the first subblock data; and

computer readable program code means for causing a computer to repeat the randomizing and the diffusing, wherein at least two bits of the randomized data is reflected on one bit of data to be randomized next.